UNIVERSITY OF CAMBRIDGE

Online Payment Methods

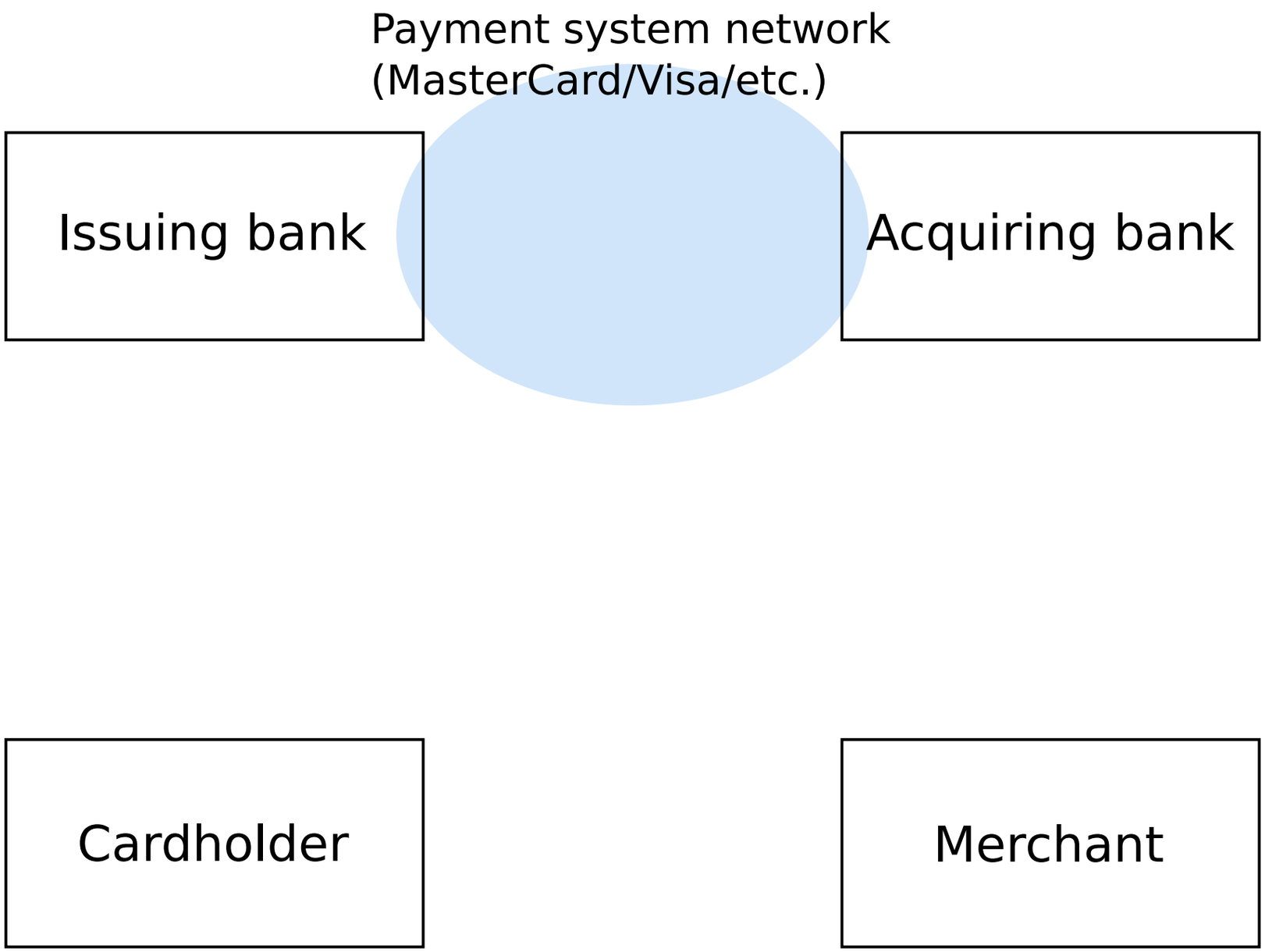
Dr Steven J Murdoch

Computer Laboratory

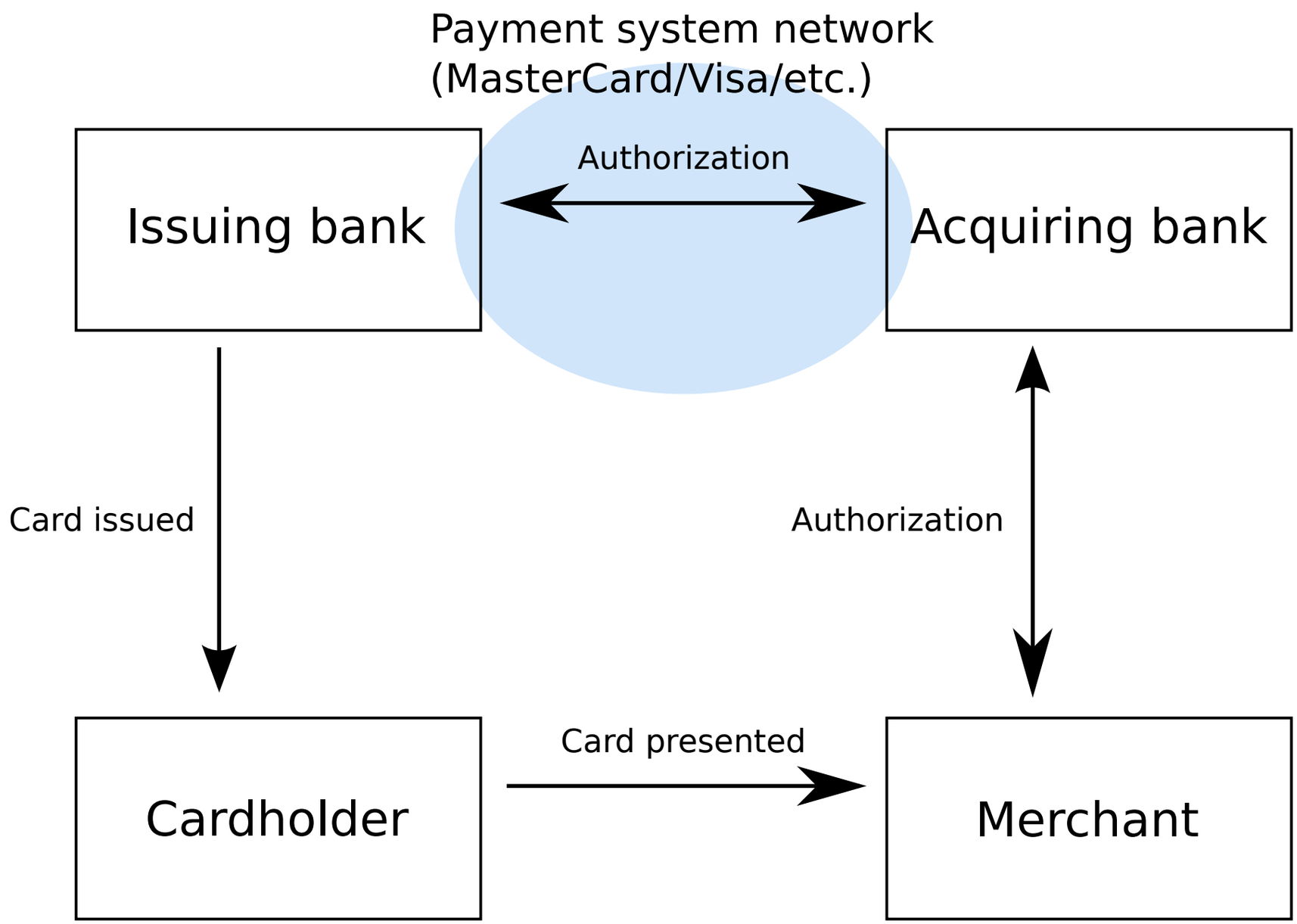
Visa and MasterCard

- What do they do?
- Some important tasks for online (and offline) payments:
  - Run communication network
  - Set standards
  - Manage disputes between members
  - **Set contractual terms between members**

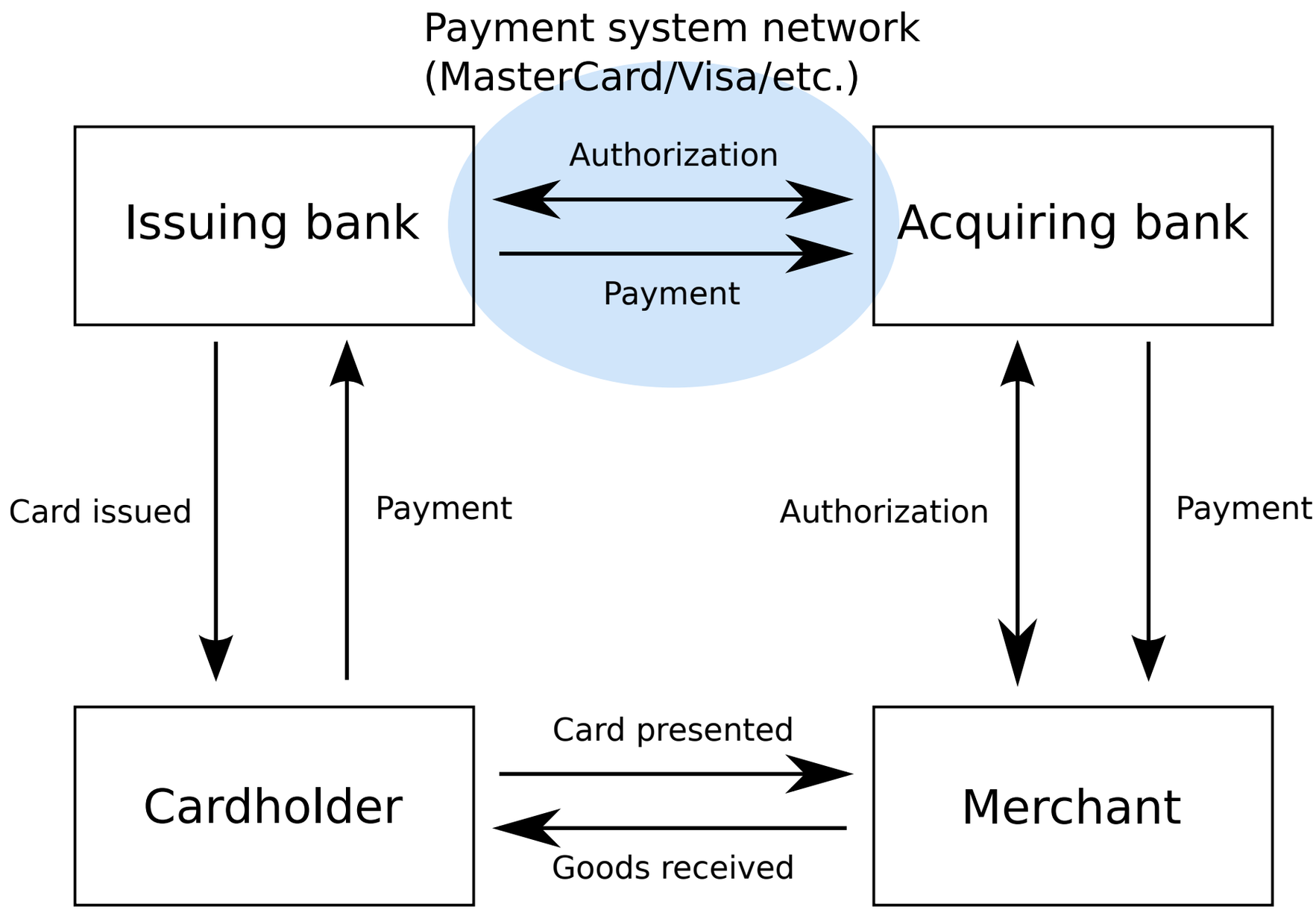
Terminology



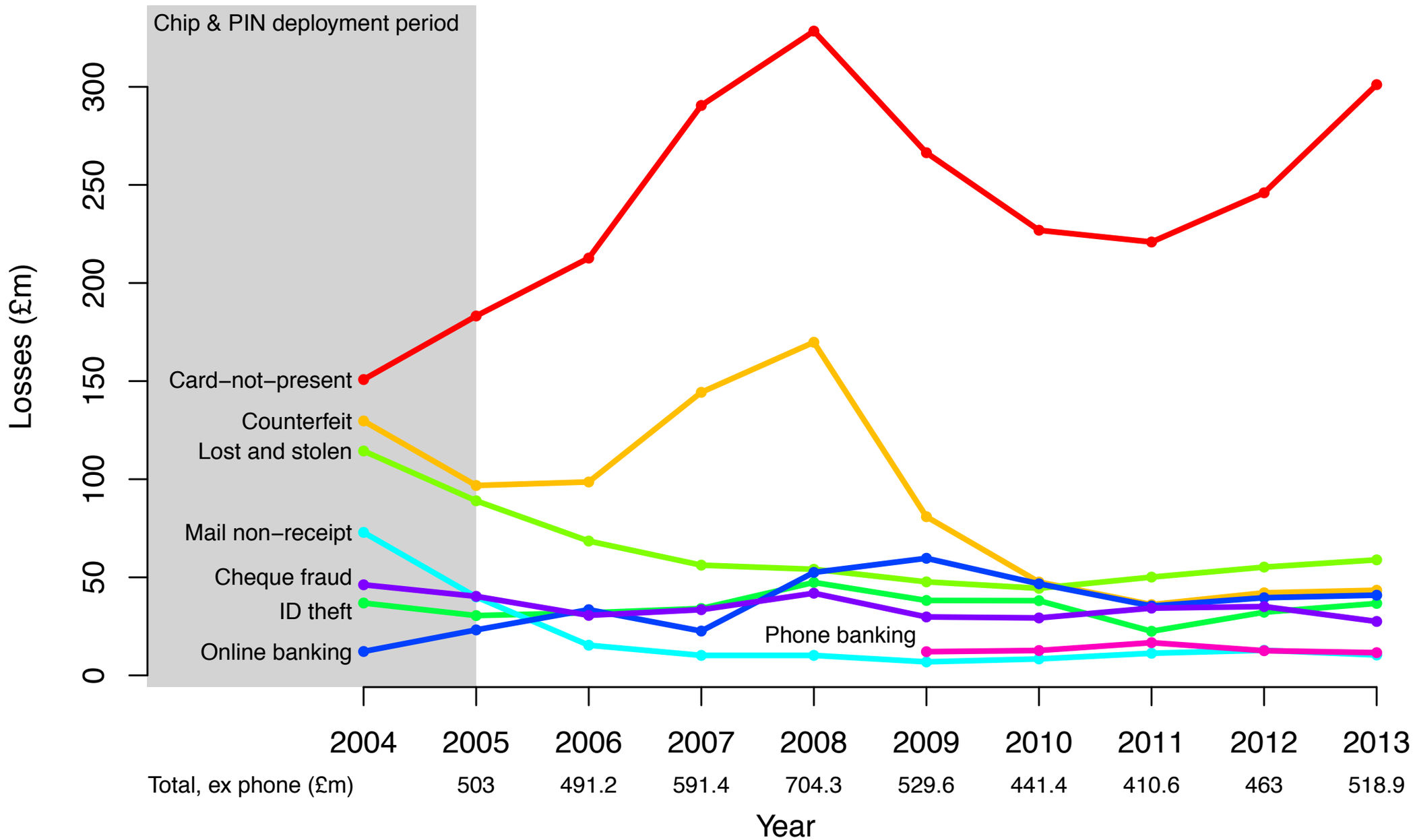
Terminology



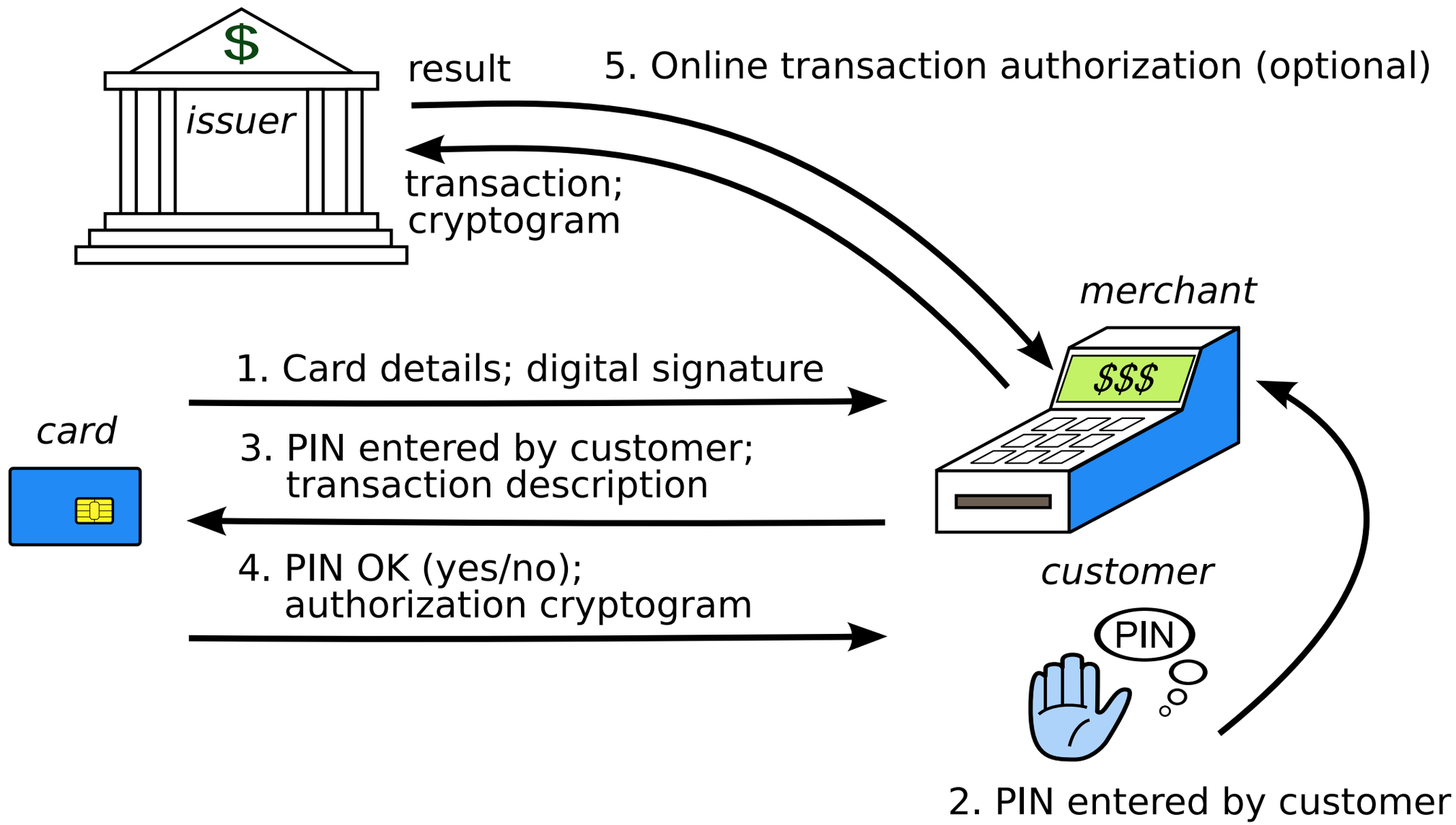
Terminology



How well does the system work?



The EMV protocol



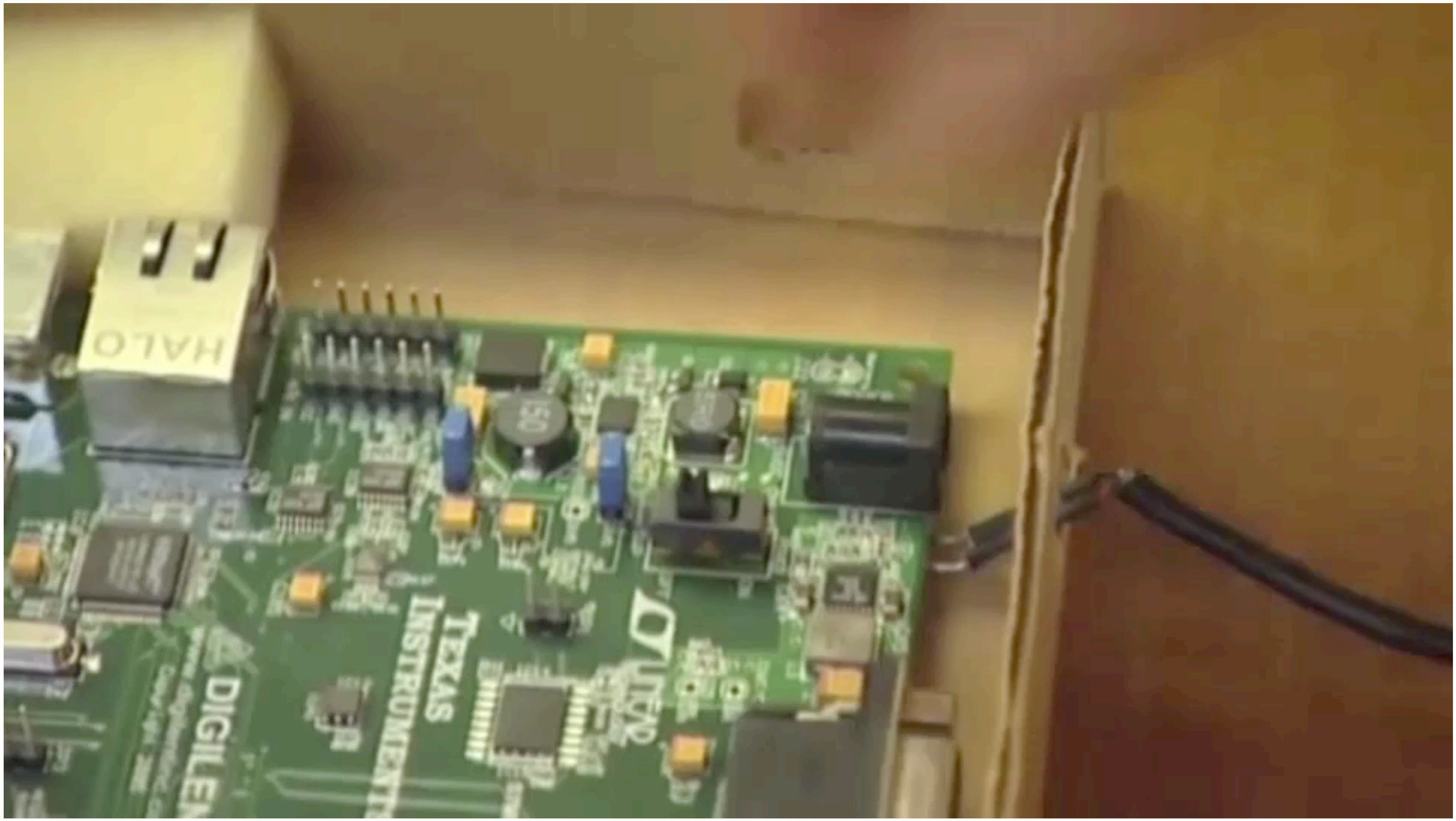
Counterfeit fraud

- Producing fake (typically magnetic stripe card) from harvested details

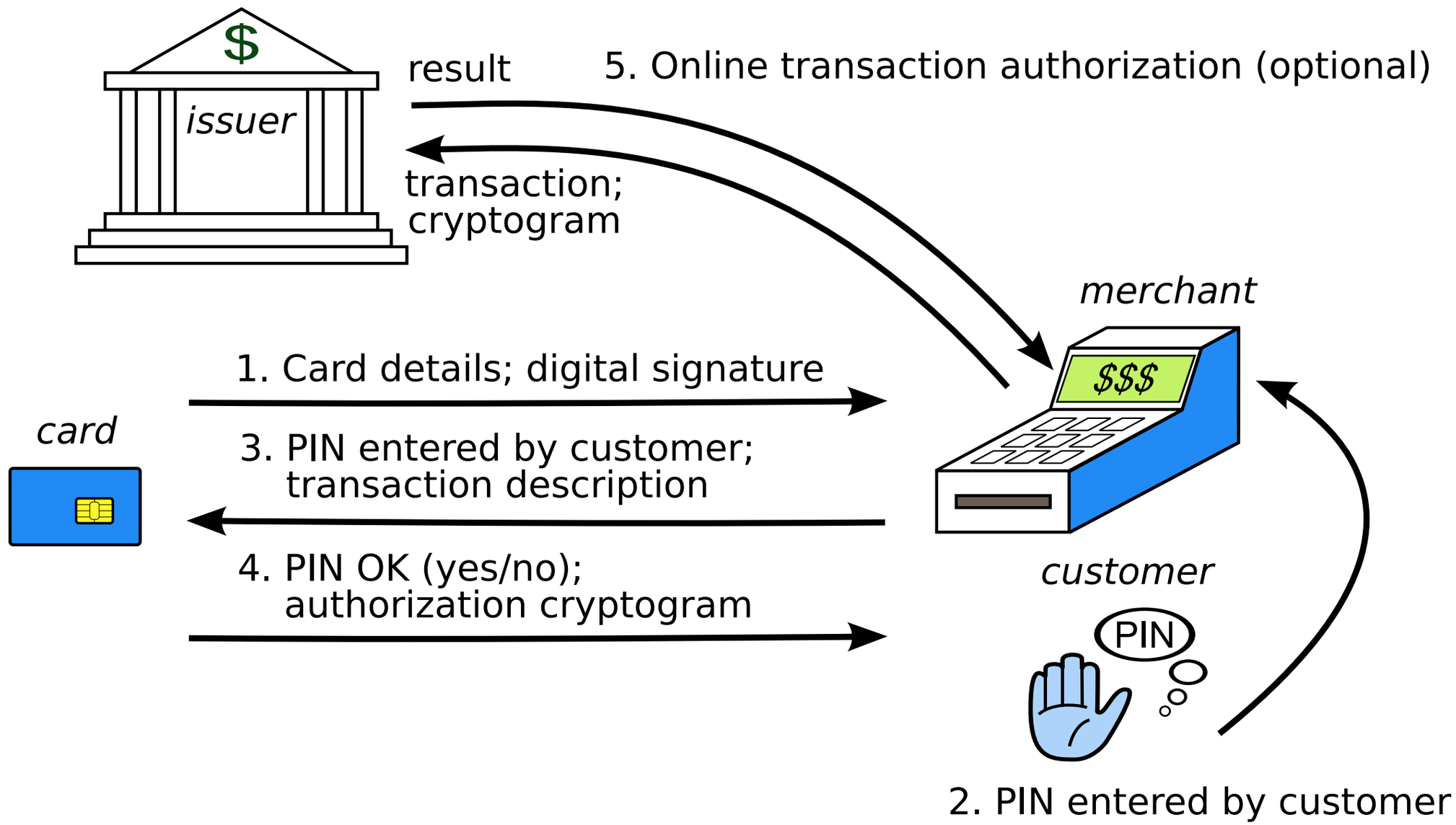
Liability engineering

	Terminal		
Card	magstrip	chip	chip & PIN
magstrip	Issuer	Issuer	Issuer
chip	Acquirer	Issuer	Issuer
chip & PIN	Acquirer	Acquirer	Issuer

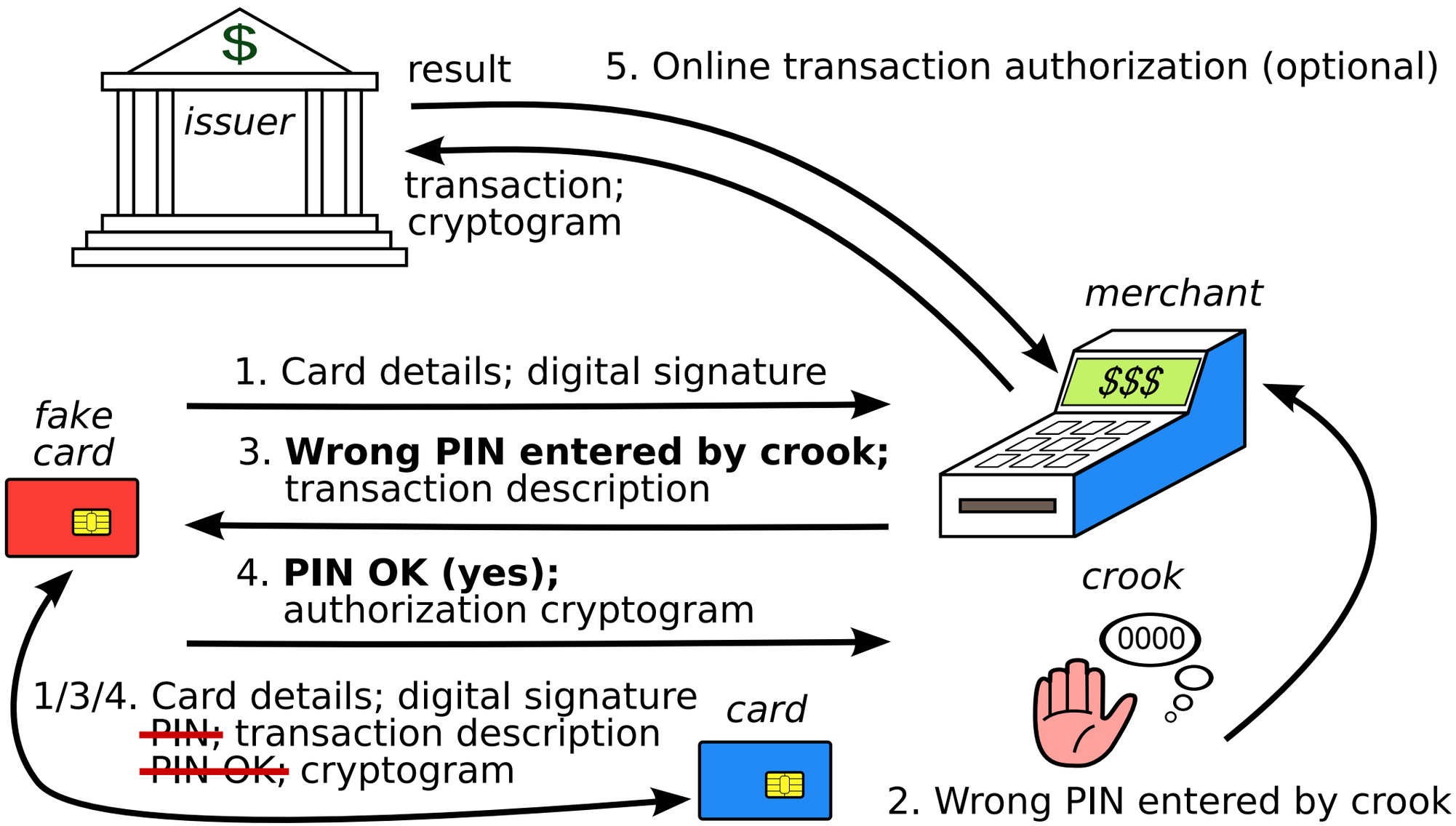
The no-PIN attack



The EMV protocol



The no-PIN attack protocol



Online banking authentication

- Simple scam is to “phish” for account details
- Ask for username and password
- Low success rate, but just a few customers is enough to make investment worthwhile
- Actually moving money out is the high-risk part of the scam
- This is allocated to money-mules recruited supposedly to pay foreign staff
- Often the money mule will lose money and may be prosecuted for fraud

Dear Customer

Account Protection Update, To ensure th
scam and other account threats, it's strc
update account protection
click on "Protection" to continue the proc

Protection .

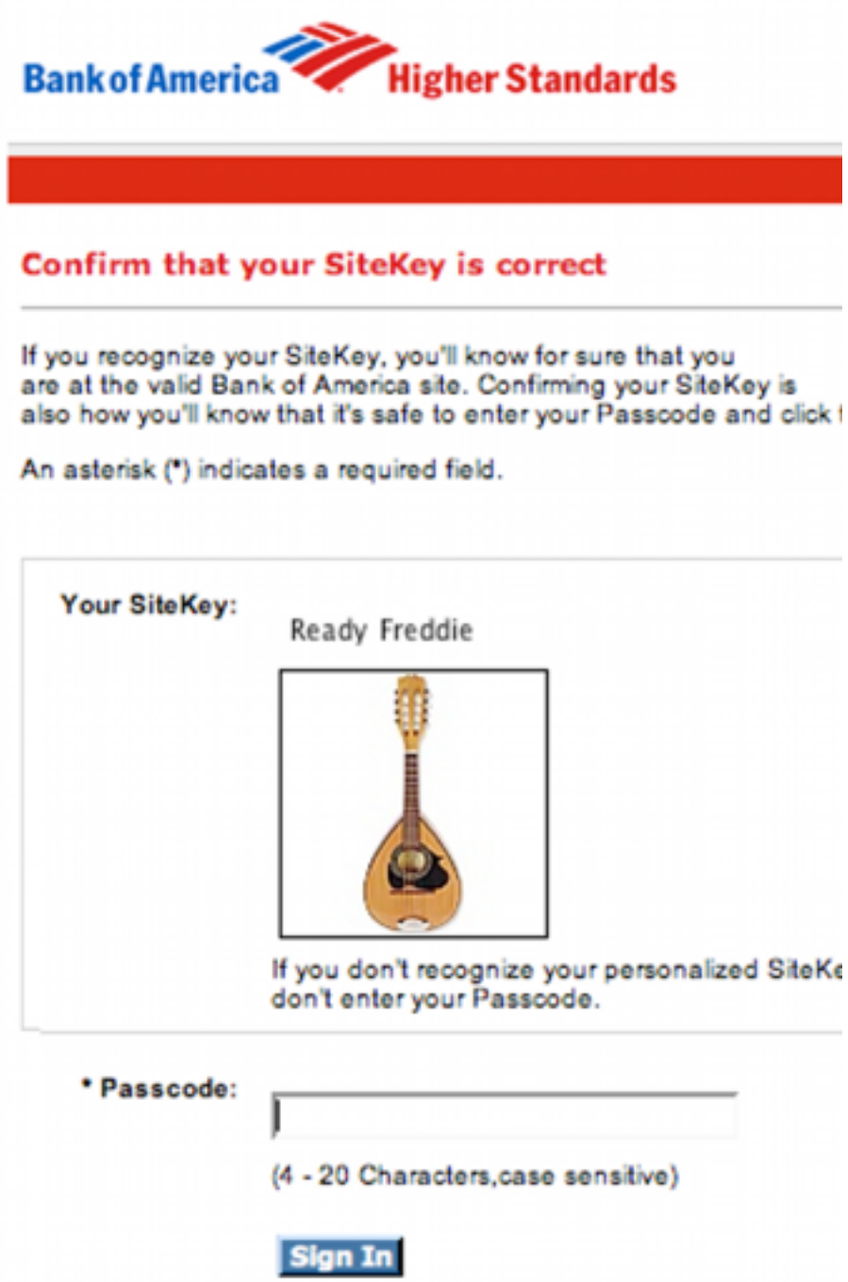
Online Internet Banking Security Center
Halifax Internet Banking.

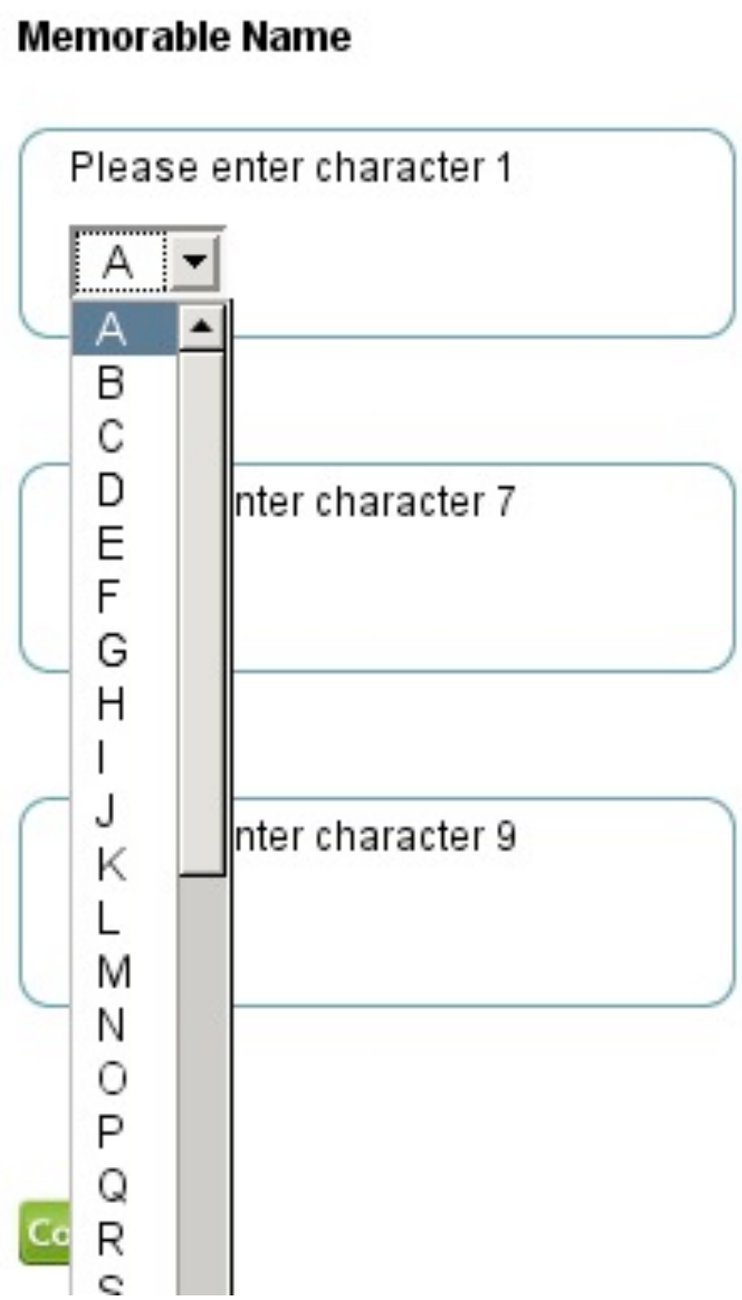
Thanks for your co-operation.

Fraud Prevention Unit
Legal Advisor
Halifax PLC.

Please do not reply to this e-mail. Mail sent to this address

Hardening passwords





Replacing passwords (iTAN)

Empfänger:
Max Mustermann
Konto-Nr. des Empfängers: 123456
Bankleitzahl: 55555555
Bei Kreditinstitut: Testbank
Betrag in EUR: 1,23
Verwendungszweck 1:
Verwendungszweck 2:
Konto-Nr. des Auftraggebers: 4720
Ausführungsdatum (TT.MM.JJJJ): (Optional)
Auftraggeber: Mustermann
Als Vorlage unter folgendem Namen speichern:

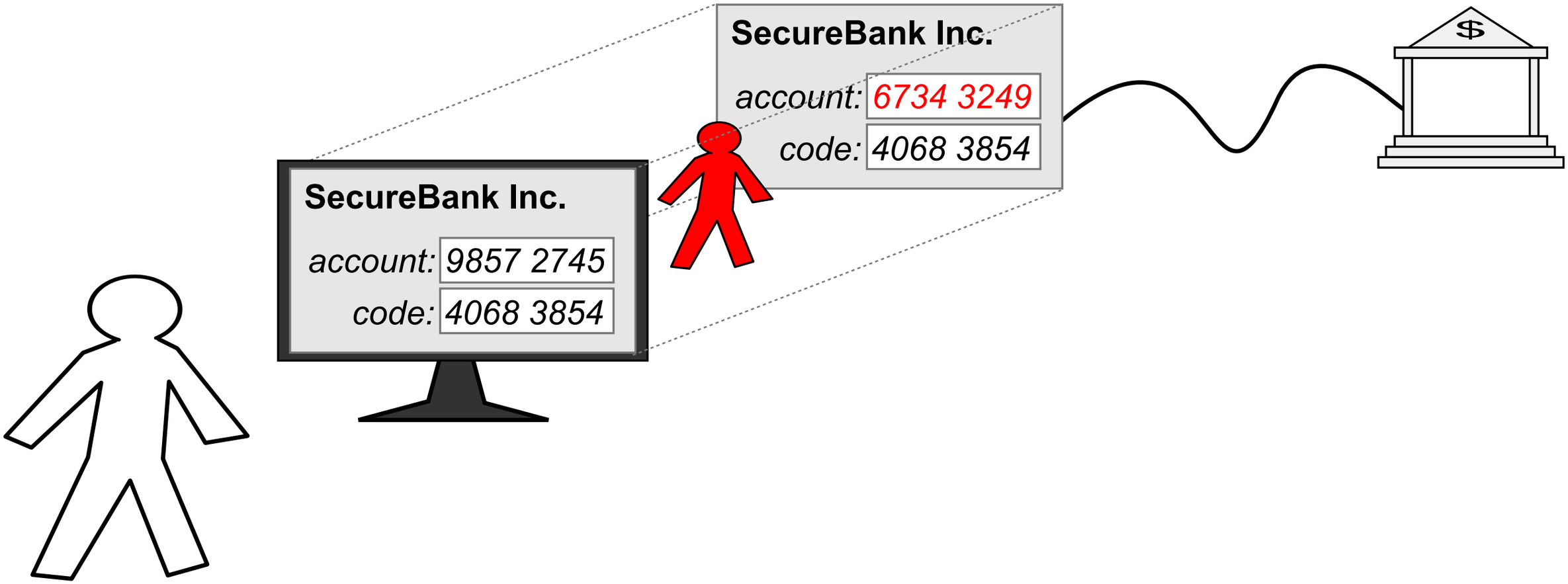
Bitte geben Sie die TAN neben der Nummer 35 ein: 533098 OK

TAN-Nummer

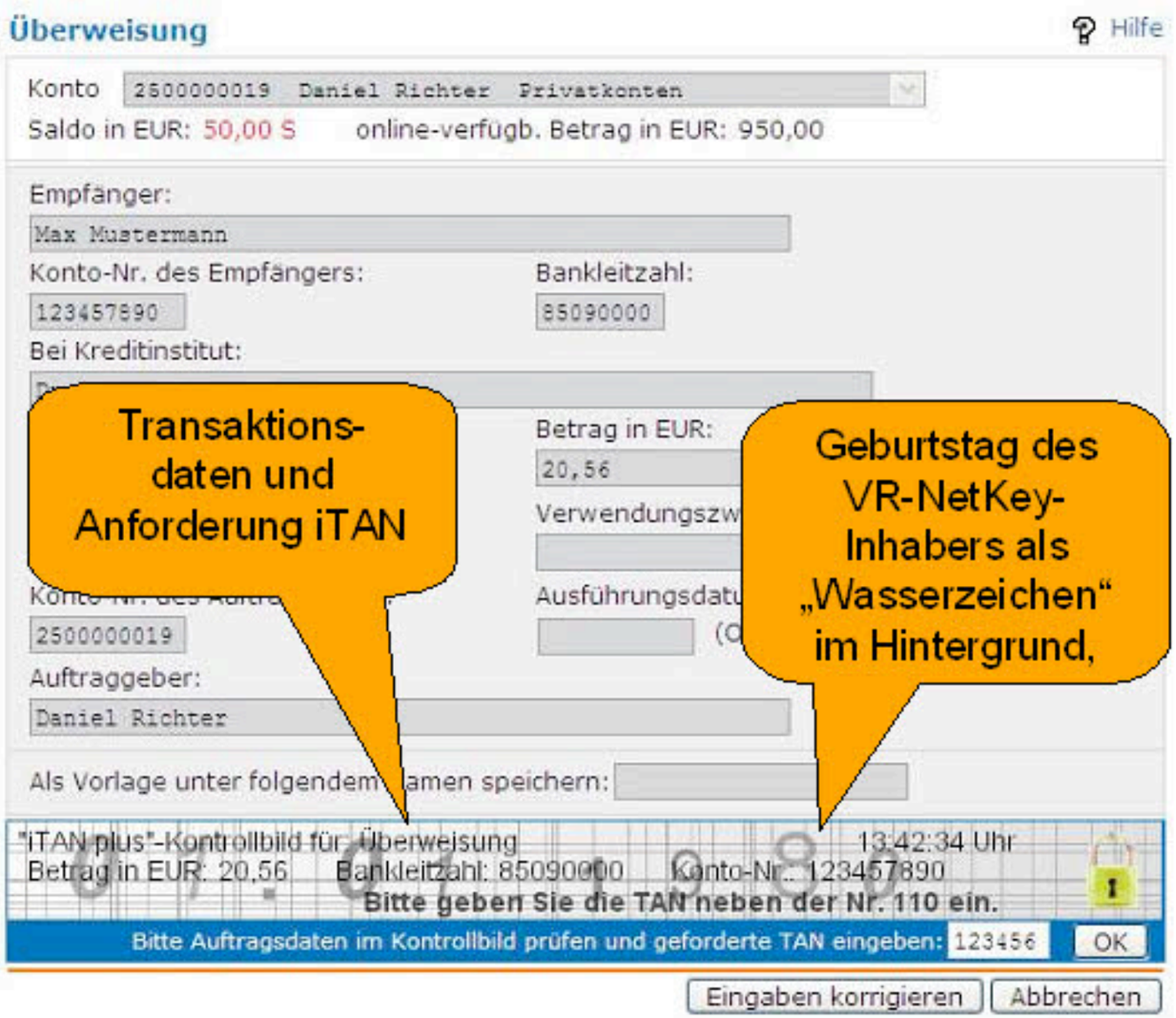
Nr.	TAN	Nr.	TAN	Nr.	TAN
1	687716	31	842387	61	723733
2	143690	32	559269	62	164612
3	908192	33	900420	63	491715
4	150266	34	950912	64	858265
5	637410	35	533098	65	500439
6	632961	36	734080	66	832015
7	028567	37	872269	67	046584
8	179016	38	301940	68	212578
9	888375	39	038797	69	784722
10	606687	40	780513	70	115323
11	051256	41	807036	71	040492
12	647111	42	085357	72	637365
13	529030	43	508000	73	470604
14	844281	44	781571	74	217050
15	714399	45	484862	75	790635

Laufende Nummer (Index)

Man in the Browser



MitB protection



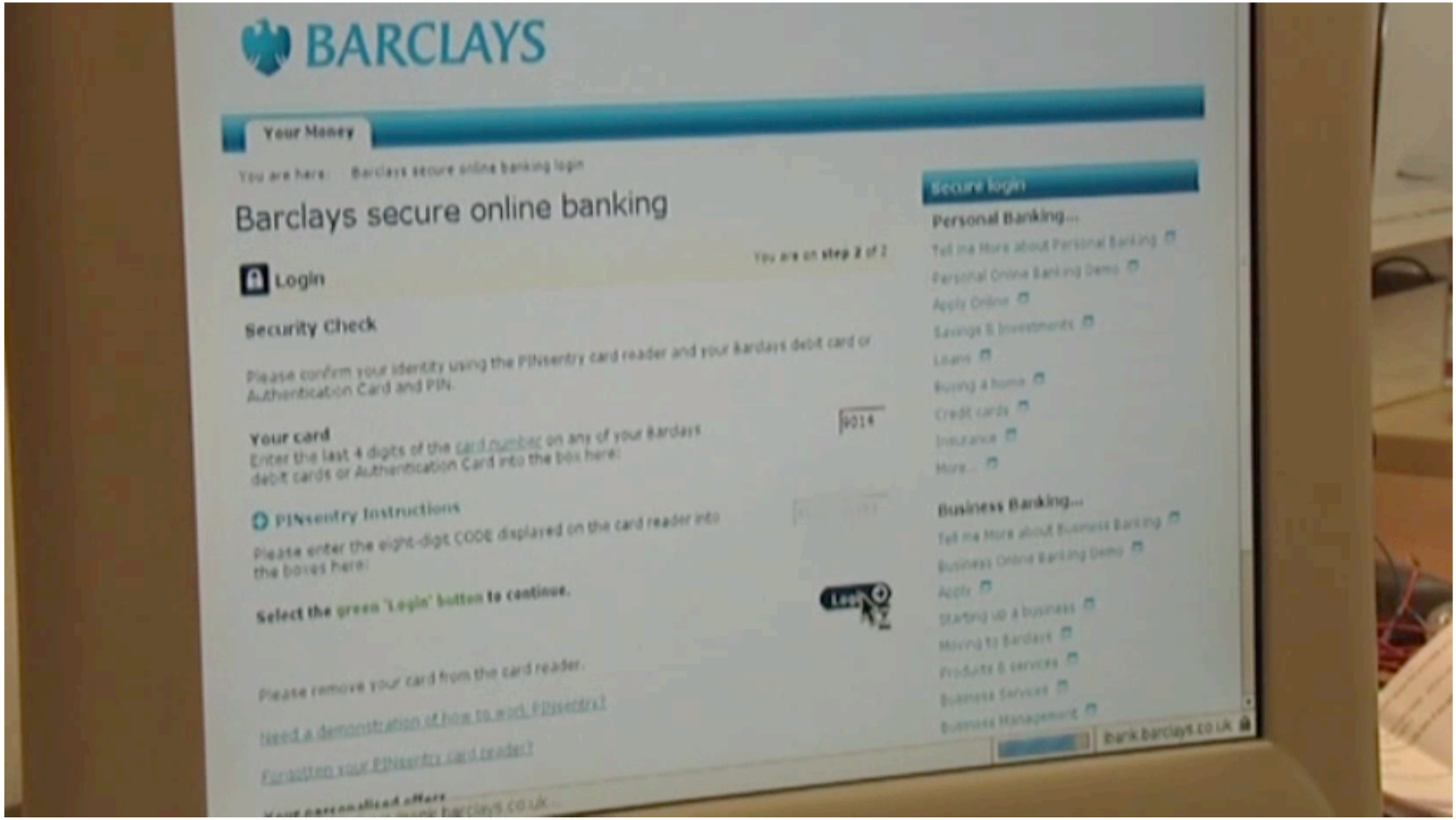
Transaction authentication

Summary so far

- Counterfeit fraud
  - Magnetic stripe fallback facilitated by Chip and PIN
- Lost and stolen/Mail-non-receipt
  - no-PIN attack can bypass PIN protection
- Cheque fraud and ID theft
  - Primarily not a technology problem
- Online banking
  - Transaction authentication likely the way to move

Combining EMV with online banking

Combining EMV attacks with online banking



Card not present transactions

- Basic version: same as old card-present transaction
  - Card number and expiry date sent back
  - Can also send back CVV2 off back of card
  - Can also perform address verification
- Every extra step will lose customers at check-out stage
- Some vendors will skip security measures
  - Amazon don’t even perform CVV2 checks
  - Leaves non-Amazon users at risk of fraud (though will eventually be refunded)

Acquirer interface for web based merchants

- Small web merchants will not deal directly with acquirer
  - To allow international payments, many acquirers likely needed
  - Merchants might like to avoid access to customer details as much as possible to reduce liability
- Examples of payment processors include
  - Sage Pay
  - Worldpay
- Paypal slightly different
  - Hoped people would leave money in account; actually mostly ended up as payment processor

Example: Sage Pay (Form)

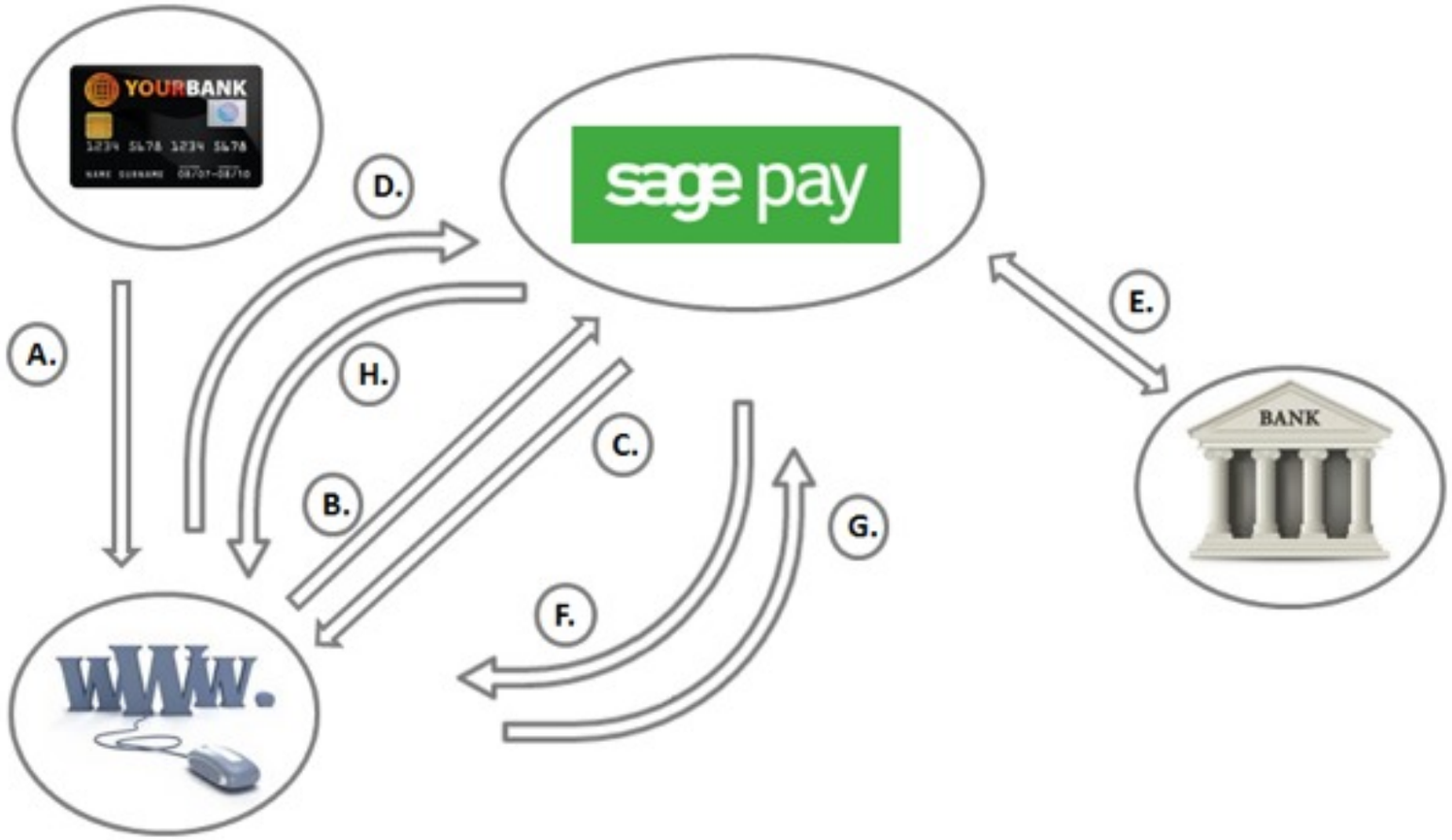
A. Shopper visits your website to make a purchase.

B. You re-direct your shopper through to our payment pages.

C. We capture the details, and pass these through to the bank for authorisation.

D. We send your shopper back to your Success or Failure page with the transaction results.

Example: Sage Pay (Server)



A. Shopper visits your website selects the item, and enters their details on your website.

B. You send the details of the transaction to us using our protocols.

C. We validate all of the details, and pass you the "Next URL" for you to transfer your shopper.

D. You transfer your shopper from your website through to our payment page.

E. We capture the card details, and send these to the bank for authorisation.

F. We notify your system of the status of the transaction to your Notification URL.

G. You respond to us with your re-direction URL.

H. We send your shopper back to your website where they are told the status of the transaction.

Example: Sage Pay (Direct)

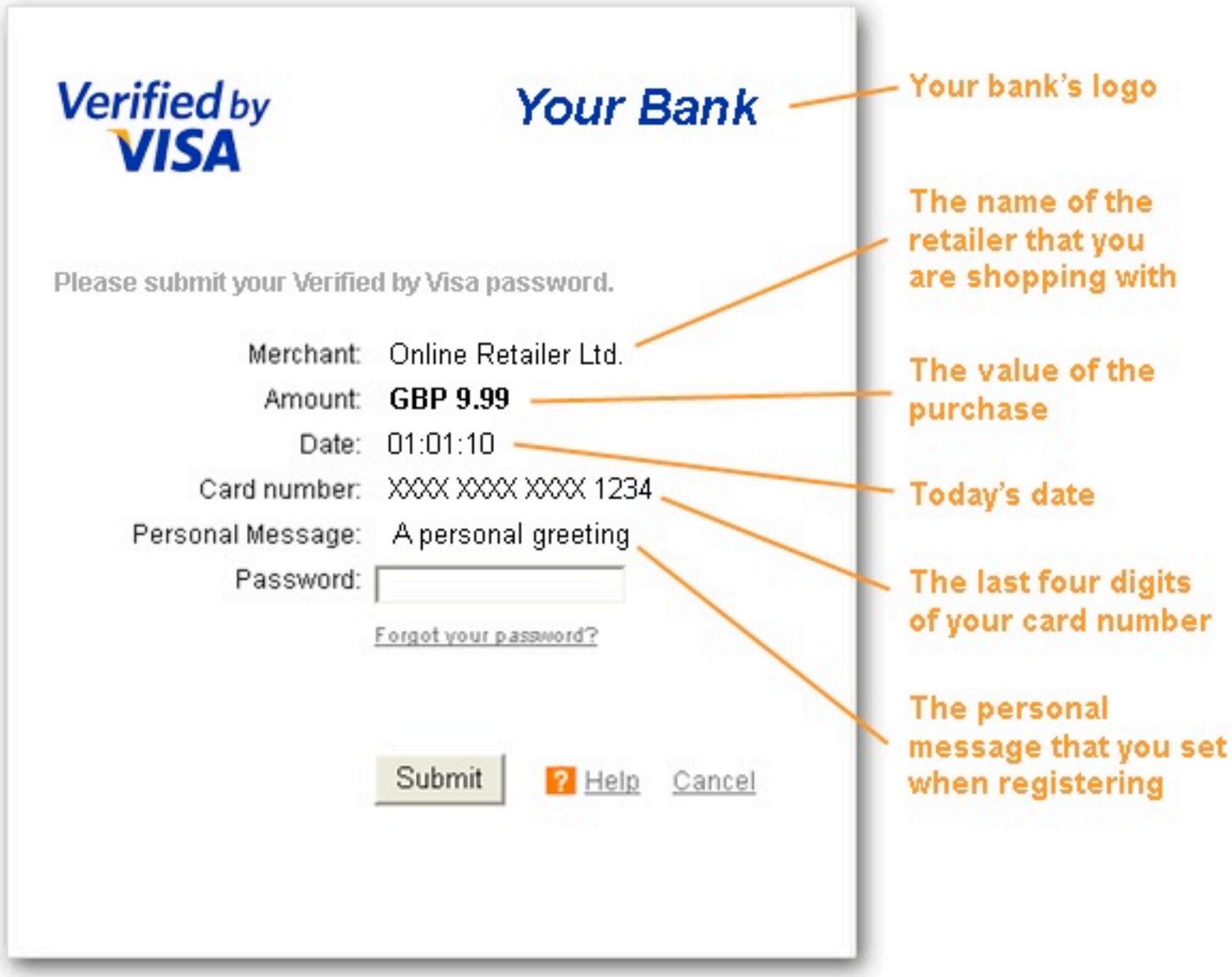
A. Shopper visits your website selects the item, and enters their card details on your site.

B. You send the details of the transaction, and the card information to us using our protocols.

C. We validate all of the details, and pass these through to the bank for authorisation.

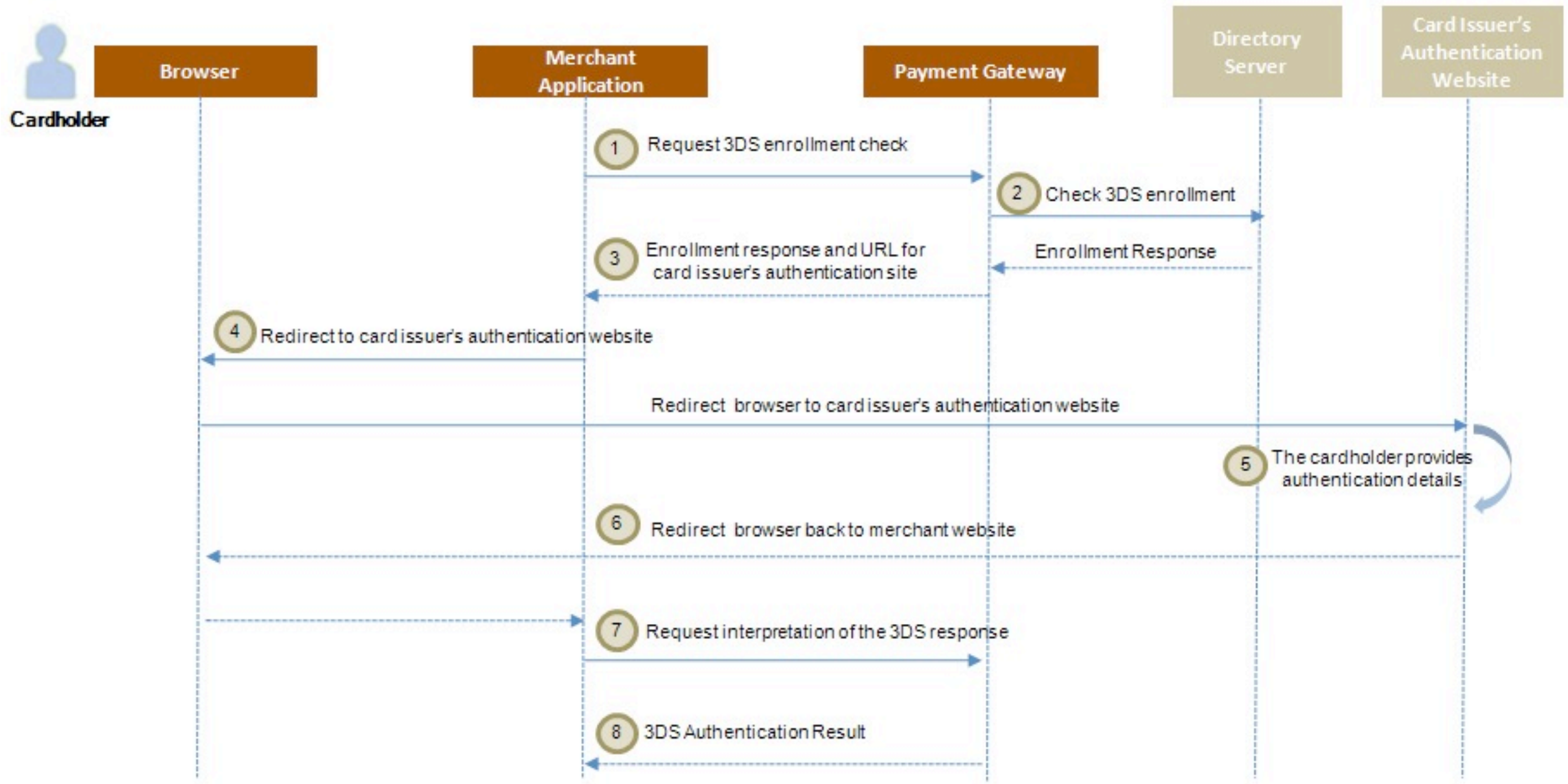
D. We send you the status of the transaction which you then display to your shopper.

3-D Secure (Verified by Visa/MasterCard SecureCode)



Visa

3-D Secure (Verified by Visa/MasterCard SecureCode)



American Express

3D secure phishing vulnerability

Verified by VISA

MasterCard SecureCode

Verified by Visa / MasterCard SecureCode Enrollment:

Due to recent changes to FDIC Deposit Insurance Rules all our customers must be enrolled in Verified by Visa or MasterCard SecureCode program depending on type of your Check Card. **To continue complete this form and click Activate Now.**

Social Security #: - -

Card Number: (16 digits)

Expiration Date: / (MM/YY)

Signature Code: (Last 3 digits on the back)

Card PIN Code: (4-6 digit code that you enter in ATM)

Choose Password: How will it be used?

Confirm Password: (6-12 characters lenth)

Activate Now

If you already enrolled in Verified by Visa or MasterCard SecureCode program to continue please enter current password or select new then **click Activate Now.**

VERIFIED by VISA

Welcome, 00034-5432-PSI-54256

Verified By Visa

Enter Account Information

Please enter the information below and click the "Continue" button. You can review this informa
verified by visa account..

Payment Information

Tell us the card to add to your Account.

Card Nickname (example: My Bank One Visa)

Card Number

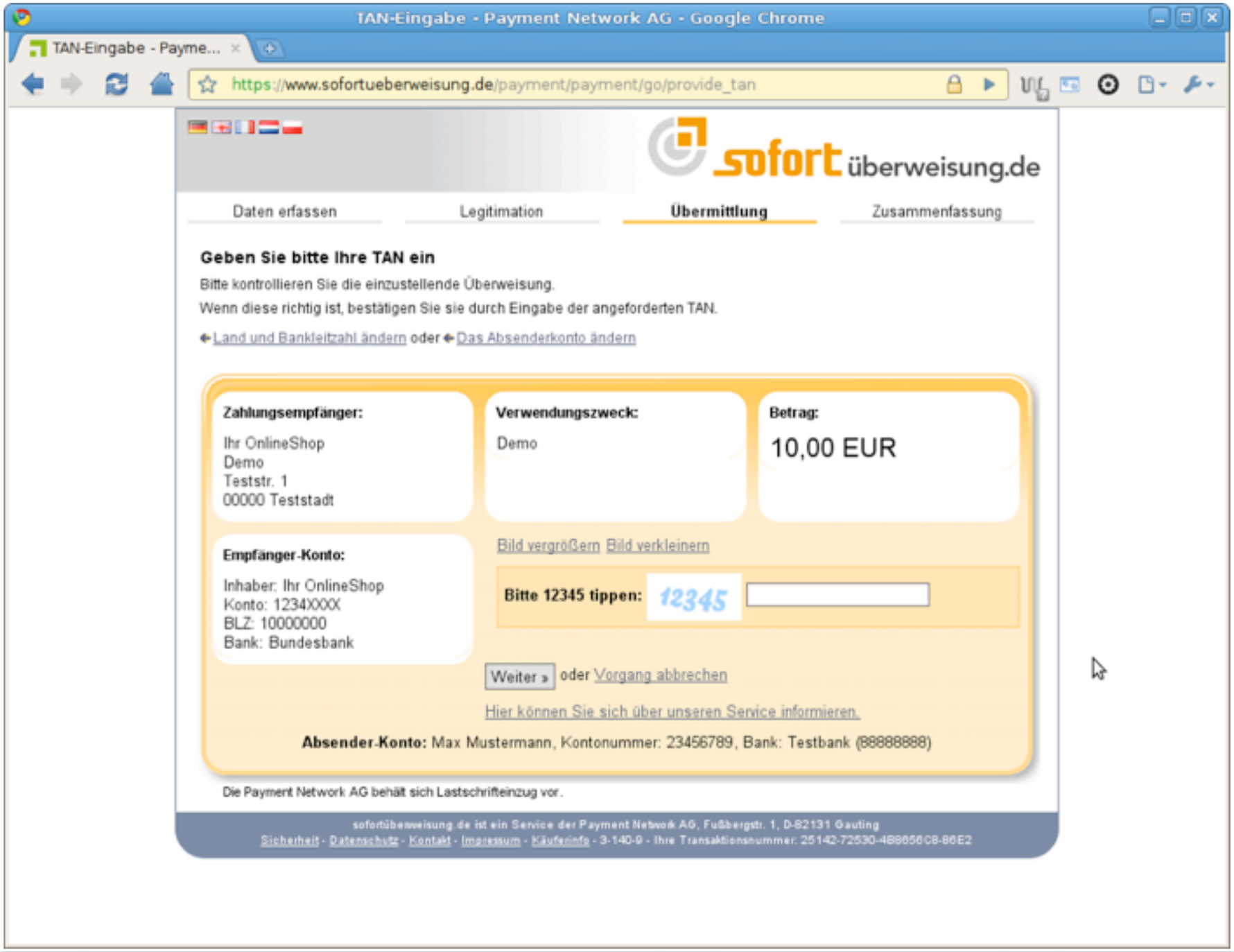
Expiration Date

CVV2

ATM Pin

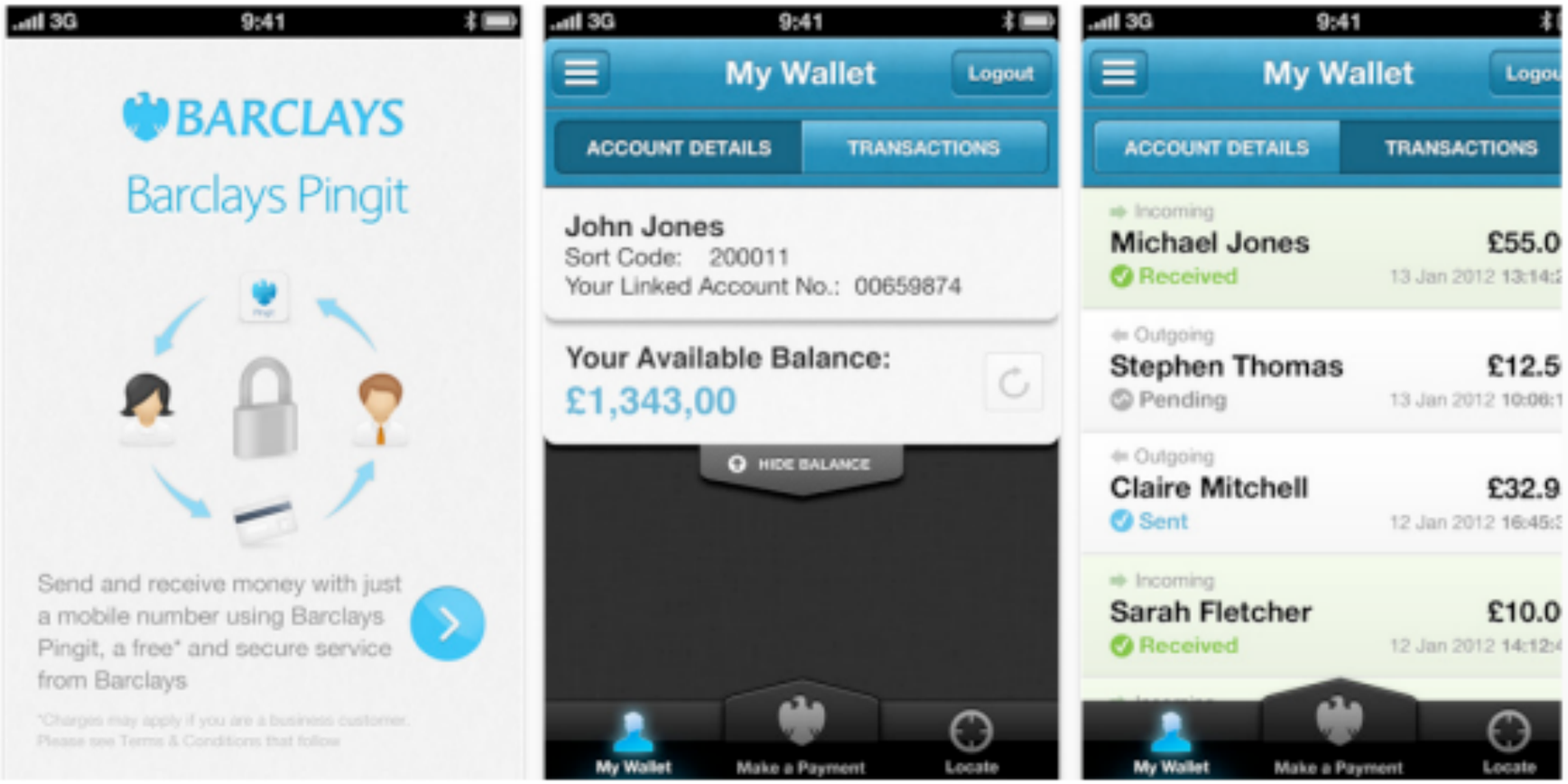
Name on Card (first/last)

SOFORT Überweisung



Mobile payments

- May just be interface to online banking website
- mPESA and similar use mobile SIM as root of trust (serves underbanked)
- Barclays Pingit based around Direct Debit



Summary and conclusions

- For card-present transactions, Chip and PIN was supposed to help
  - Reality was more complex and fraud went up
- Card fraud is now dominated by card-not-present transactions
  - Merchant pays cost, but extra security loses customer conversions
  - For small merchants, much of the work is delegated to payment processor
- Online payment systems typically run on previous rails
  - Credit/debit card (optionally with 3D Secure)
  - Online banking
  - Direct debit